Copy to DD(ESA)
18/9.

15(L)

Interrogation of Herr REINHARD WAGNER (OKW/CHI) On Japanese Systems.

Herr REINHARD WAGNER was interrogated on 22nd August 1945 at his home in NIEDERRAMSTADT near DARMSTADT, Ringstrasse 4, by Captain James K. LIVELY, whose report is attached. In the information brief provided by TICOM it was stated that WAGNER, an Obergefreiter discharged from the OKW, had knowledge of the Japanese language and cryptographic systems.

TICOM

No.of Pages. 4.

13/9/45.

Distribution.

British

D.D.3
D.D.4
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
Miss Mortimer (2)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan

U.S.

OP 20-G (2) (via Lt.Cdr.Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (2) (via Major Seaman)
Director, S.I.D: USFET
(via Lt. Col. Johnson)
Col. Lewis Powell

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt. Col. Johnson
Lt. Cdr. Manson
Major Seaman
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Personal data.

WAGNER was born on 14th July 1907 in HALLE/SAALE, the son of a parson. He was educated in HALLE, attending the gymnasium in that city and studying the humanities. He then pursued a course in theology at HALLE, TUEBINGEN and MARBURG. After completing his theological studies, he broke with the Evangelical Church and joined the Christian Community (Christengemeinschaft), a confession midway between Evangelicism and Catholicism. He held pastorates in ROSTOCK, from 1926 to 1934 in LEIPZIG, and from 1934 to 1936 in CHEMNITZ. From the summer till autumn of 1936 he was in JAPAN where he began his study of the Japanese language - a study which he has continued since. He returned in the fall of 1936 to VIENNA where he again engaged in pastoral activities. He claims domicile in VIENNA at the present time. In 1941 the Christian Community in VIENNA was abolished by the Gestapo. On 1st August 1941 WAGNER was inducted into military service. He was trained originally in the medical department, but on 8th October of the same year was transferred to OKW/Chiffrierstelle, BERLIN, Bendlerstrasse 33. He was employed in Referat 13 under Oberleutnant ADLER, a referat which studied Chinese and Japanese crytographic systems. WAGNER however worked only on Japanese material. In addition to being a language specialist, he was active in recovering code books and in solving crytographic procedures. Associated with him were Dr. SLAWIK, Dr. SCHMAHL, Obegf. MAJLAT and Fraeulein DEHN, who were however all language people. WAGNER was according to his statement the only analyst. He knew no people in other Referats since German security requirements forbade crypto personnel to associate with their colleagues in other branches. WAGNER stayed with OKW/Chi from 1941 till the end of the war at which time the referat had moved to the vicinity of WERFEN/SALZBURG.

General Scope of WAGNER's Knowledge.

The only Japanese systems which Referat 13 of OKW/Chi studied were diplomatic. They were unable to read any Army, Air Force, Navy or weather codes. He does not know what may have been done with regard to those types of system at OKH/Chi, OKM or RLM/Fa, since as far as he could tell there was no liaison between these agencies. Further, the only Japanese systems which they could read were hand systems. Up until the outbreak of the European war in September and prior to WAGNER's entry into the referat, they could read a machine system (designated by the referat only as "die Maschine"), but at that time the Japanese made changes in the system and it could no longer be read. Referat 13 did not make use of HOLLERITH or other types of machines in cryptanalysis.

Synopsis of Japanese Systems.

WAGNER described the following cryptographic systems.

(1) LA - code. LA was the Japanese indicator (Kennwort) in the text. This was a 2 and 4 digit code unreciphered. It had no security whatsoever and served mainly as an abbreviation code. WAGNER compared it to Mosse or Bentley code. The system remained in use by the Japanese till the end of the war. It was fully recovered by OKW/Chi.

(2) KOKOK - code (Japanese Kennwort). The code was a 2 and 4 letter code. Reciphering process was transposition on the basic of a repeating 19-digit keyword (Losung). This system was dropped 1st January 1942, having been solved up to that time.

/(3)

(3) A transposition procedure (Wuerfelverfahren), on which WAGNER did not work himself and which he knew only through having translated messages passed in the system. He could say of this system only that there was a daily changing keyword, and the reciphering process was complicated by Raster. The system remained valid until August 1943.

(4) The successor to the above transposition procedure, which WAGNER helped to solve, employed a basic 2 and 4 letter code book. Transposition was done in a width of 25 and a depth of 10. The keyword was changed arbitrarily. Not all the fields in the transposition square were employed but gaps (Loecher) were left. For example, the first square in the first column was to be left blank, the second square down in the second column, and so forth up to ten. In the eleventh column the top five squares down might be left blank, and in the twenty-first column the bottom five squares.

In January 1944 the procedure was complicated by causing blank squares to be left vertically and horizontally. E.g., in column one, starting from the top down five squares were to be left blank. In column two, starting with the second square down, five squares horizontally were to be left blank. In column three, starting with the third square down, five squares vertically were to be left blank, etc. The referat was successful in breaking this system.

(5) The machine. When W. first came to the referat, he heard of a machine system which had been read up until September 1939. In his opinion, based on hearsay evidence only, the machine had two wheels, one with six letters, the other with the remaining twenty. When the European war broke out, the machine was changed and traffic could no longer be read.

(6) Additive system. WAGNER thinks that this system was compiled at a powwow held during the summer of 1943 at Ambassador OSHIMA's house. It made use of a simple four figure basic code with 1200 values. Reciphering was carried out with an additive book of 400,000 additive values, each page of the book being drawn up 20 x 25. The point at which the encipherer started to use the additive was indicated by a Kenngruppe, e.g., TLUSR. WAGNER believes that there was a large index which would show the page and line to which a given Kenngruppe referred. The encipherer always started with the first group at the left and proceeded to the right.

After the additive procedure was completed, the figures were converted to letters, the same letters always representing the same numbers.

(7) Transposed code. Between BERLIN and TOKYO passed a sizeable volume of economic traffic which was encryptographed by transposed code. There were four codes, designated AHSAJ, ETGAV, AMNUM and IINIM. AHSAJ was a 3,4,6 letter code, ETGAV a 6 letter, AMNUM 5 letter, and IINIM was unknown to WAGNER. Each code contained 10,000 values altogether. Of those on which WAGNER had worked perhaps 4 or 5,000 values were recovered.

There were two reciphering processes, CIFOL employed on even days, VEVAZ employed on odd days. Reciphering was a matter of transposition, employing not only blanks (Loecher) in the transposition square but also irrelevant filler-text (e.g. "Today it is raining hard") inserted to complicate the cipher text (Ausfuellungsgruppen).

(8) ABABA, BCBCB, CDCDC, etc. This was a system employed in Far Eastern traffic between JAPAN and BURMA, the PHILLIPPINES, etc. A very primitive basic code was used, and reciphering was by means of transposition (width 10, depth vague). The various Kennwoerter indicated the sequence of rows or columns. This traffic was not read after New Year 1944 owing to atmospheric disturbances which prevented intercept.

(9) WAGNER mentioned a minor system used by SATO, OSHIMA's counterintelligence man, to pass messages which SATO did not wish to come to the attention of the Ambassador. Although intended as a Top Secret system, it was exceedingly crude. Each letter of the alphabet was represented by two figures. Resulting cipher text was then reciphered by a repeating additive consisting of only ten figures which never changed.

Assessment of subject.

WAGNER seems alert, intelligent and cooperative. He would like to obtain employment with the U.S. cryptanalytic services to continue his work on Japanese material.

On the basis of advice available and information known to the interrogator it would not appear that WAGNER has knowledge not already possessed by U.S. or British signal intelligence agencies.